Poznámky z počítačových sietí - matroš na štátnice

Peter Csiba, petherz@gmail.com, https://github.com/Petrzlen/fmfi-poznamky

15.06.2012

Obsah

Úvod. Text je poznámkami k oficiálnym štátnicovým otázkam a boli spísané počas učenia sa na ne. Poznámky sa nesnažia ísť do hĺbky (na to je Tanenbaum, RFC a Wikipédia). Naopak, snažia sa priniesť intuitívnu predstavu o technológiách a dávať jednotlivé pojmy do súvisu.

Poznámky sú organizované podľa štátnicových otázok, snažia sa minimalizovať omáčku a nevysvetlujú a neuvádzajú do problematiky[1]. Text je určený čitateľom, ktorý sa už s hlavnými pojmami stretli. Ďalej autor odporúča čitateľovi si pozrieť hlavne detaily konkrétnych TCP/IP protokolov, ako napríklad IP, UDP, TCP, SSL/TLS alebo DNS.

Autor neabsolvoval prednášky ani test z predmetu Počítačové siete a nemá skúsenosti s ich administráciou. Nemenovaný prednášajúci ohodnotil znalosti počítačových sietí autora pred písaním textu na D+[2], takže autor aj preto neručí za korektnosť textu. V skratke, čitateľ informácie z tohoto textu vstrebáva na vlastné riziko :).

Nakoniec poznamenajme, že autor sa snažil písať pravdu a len pravdu, keďže jeho odpoveď na záverečných skúškach vychádza z tototo materiálu. Ak čitateľ chce prispieť ku kvalite textu, nech autorovi napíše a ten mu udelí prístup do repozitára.

1 Telekomunikácie

1.1 Koncept prenosu informácií

???

1.2 Integrácia

???

1.3 MPLS (Multiprotocol Label Switiching)

Medzi 2. a 3. vrstvou OSI ("layer 2.5"protocol). Podporuje priame spojenia, aj circuit based (na viacero skokov). Hlavička (label) sa skladá z adresy na linkovej vrstve. Hlavičky môžu tvoriť stack, čím sa umožňuje posielať datagram cez viacero liniek.

Navrhnutý 1996, podpora pre väčšinu linkových a dátových protokolov. Unifikuje prístup k nim.

2 Základné pojmy zo sietí

2.1 Topológia a geografia

Topológia - organizácia siete. Fyzická (aká je v skutočnosti) a logická (ako sa správa). Nemusia byť rovnaké, napr. zariadenia spojené Ethernetom a hubom majú fyzickú topológiu hviezdy a logickú topológiu zbernice (lebo posielaný signál počuje každý).

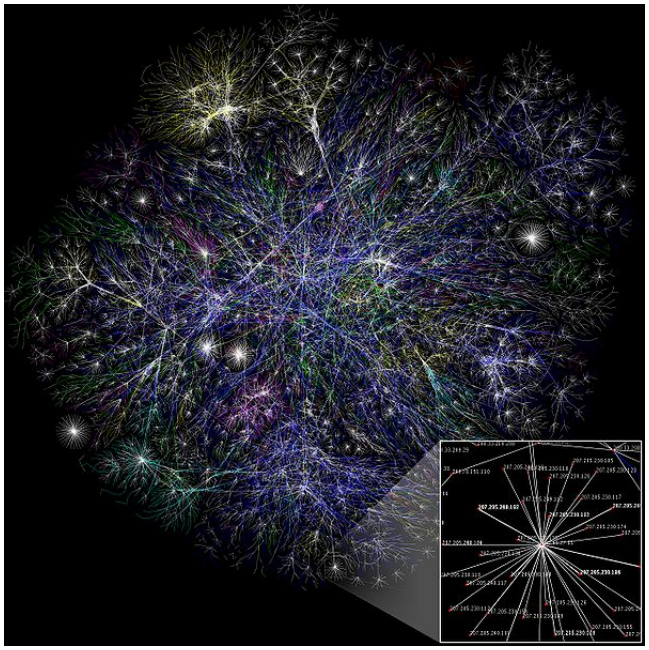
- Point-to-point - dve zariadenia spojené priamo.
- Zbernica (bus) - viaceré zariadenia pripojené na zdielané médium. Ethernet spojený hubom, odpočúvanie telefónnych liniek alebo zbernice vnútri počítača. Na riadenie komunikácie sa používa CSMA/CD alebo CSMA/CA (collision detection a collision avoidance s exponential backoff).
- Hviezda (star) - centralizovaný prvok riadi komunikáciu. Každé zariadenie je spojené so šéfom štýlom point-to-point. Napr. router. Výhodou je, že je triviálne pridať nové zariadenie.

[1] A občas zabudol na formalizmus a tretiu osobu :)
[2] Čo autora motivovalo naučiť sa to ešte lepšie.

- Kruh (ring) - do kruhu. Obľúbený teoretický model. Signály sa posielajú v dohodnutom smere.
- Mesh - see WiFi. Každý má rovnakú úlohu.
- Kompletne spojený - Každý s každým (zjavná nevýhoda: počet spojení rastie kvadraticky).
- Strom - hierarchická štruktúra, je daný koreň stromu, medzi vrcholmi sú point-to-point (graf netvorí cyklus). Môže na ňom byť implementované smerovanie (routing).
- Hybrid - napr. Internet.
- Daisy chain - spojenie viacerých zberníc, ktoré môžu tvoriť cyklus.

Kategorizácia podľa geografie siete (od najmenších po najväčšie):

- PAN - Personal area network - do 10m. USB, Bluetooth, LAN párty.
- LAN - Local area network - jedna budova, škola, internát. Typicky Ethernetové káble.
- Chrbtica - Backbone - spája viacere menšie siete (podsiete - *subnets*). Špeciálne prípad: Internet backbone.



- WAN - Wide area network - mestá, štáty až medzikontinentálne.
- Internetwork - prepojenie viacerých sietí (napr. nackbone-om).

Niektoré sme vynechali.

2.2 Základné typy sietí, informačné toky

???

- Informačné
- Telekomunikačné
- Sociálne
- Neurónové, Náhodné,...

2.3 Zdroje, cieľové uzly, prepínací systém

??? Asi niečo o sieťových zariadeniach.

2.4 Jednosmerné a obojsmerné spojenia

- Obojsmerné (full-duplex). Oboma smermi paralelne, ako mobilné telefóny.
- Jednosmerné (half-duplex). Len jedným smerom naraz, ako policajné vysielačky.

2.5 Konferencie, komunikačné kanály

??? Dosť všeobecné. Konferenčné hovory boli implementované aj na telekomunikačných linkách. Jedným spôsobom boli špeciálne zariadenia - mosty - ktorým sa priradilo virtuálne telefónne číslo a na ňom sa zdielala komunikácia. Druhým spôsobom bolo (napr. v UK) pridanie špeciálneho tlačítka, ktoré umožňovalo zavolať tretiemu účastníkovy od druhého (predĺžiť tak spojenie $A \to B$ na $A \to B \to C$.

2.6 Multiplexovanie

Viacero komunikácií (protokolov, pagáčov makových) cez jednu linku. Napr. sťahovanie torrentov a pozeranie emailov naraz (resp. hranie age-a). Viac na Wikipédií.

2.7 Virtuálne okruhy (virtual circuit)

Na sieťovej vrstve sa vytvorí cesta (obojsmerná) cez zariadenia, po ktorej sa posielajú dáta (bity, signály, fotóny, ...) medzi koncovými vrcholmi. Vytvorenie spojenia zaručuje, že dáta prídu v rovnakom poradí, ako boli odoslané. Opakom sú datagramy (napr. UDP), ktoré každý kus dát posielajú cez sieť (routre) neurčito.

3 Schéma jednoduchého komunikačného modelu, sieťový software

???

3.1 Technika štrukturovaného sieťového softwaru

???

3.2 Koncepcia vrstiev, protokolov a interface

Pozri 6.3.

3.3 Virtuálna a fyzická komunikácia

??? Buď ju pozvem na večeru (fyzická), alebo si chatujem na fejsbúčiku (virtuálna - využíva viaceré spojenia na dosiahnutie point-to-point).

4 Všeobecné závery z oblasti počítačových sietí, ktoré musia byť zakomponované do vrstvovej sieťovej architektúry

4.1 Adresovanie

Identifikovanie zariadení v rámci siete. Plochá addresácia (flat addressing) - adresy sa prideľujú inkrementovaním countera (alebo tomu izomorfným spôsobom), napr. MAC adresy. Hierarchická adresácia (hierarchical addressing) - tvoria strom, napr. IP adresy (IANA prideľuje adresy kontinentom a štátom, tie prideľujú adresy ISP (Internet Service Provider, napr. Orange, T-com, ...),...) alebo telefónne čísla (keď ešte fungovali cez switche).

4.2 Pravidlá pre prenos údajov

??? Prirovnáme to k cestnej doprave.

4.3 Správa chýb

Integrita správ (checksumy), samoopravné kódy (Teória kódovania skriptá). Robí sa to skoro na každej úrovni (hlavička aj telo (payload)).

4.4 Postupnosť (následnosť) správ

V prípade point-to-point nie je čo riešiť. Ak sa dáta smerujú (routujú) cez viacero zariadení, tak nemusí byť zabezpečená, keďže môžu ísť rôznymi cestami (napr. keď sa router rozhodne predísť upchatiu na ďalšej linke). Ak je vytvorený virtuálny obvod, tak je postupnosť zabezpečená. Inak napr. TCP (14.2).

4.5 Problém rýchleho odosielateľa a pomalého príjemcu

Pozri Flow control. Rieši to napr. TCP pomocou posuvných okien (sliding windows, viac 14.2). Problém je inštanciou problémov upchania siete (môže byť dôsledkom útoku), presnejšie sa snaží upchaniu predchádzať (avoidance) ako riešiť vzniknuté (detection).

4.6 Neschopnosť akceptovať správy ľubovoľnej dĺžky

Napr. ∞ dĺžky :) Konkrétnym prípadom je získanie MTU (maximum transport unit) v IP paketoch. Nie všetky zariadenia vedia spracovať ľubovoľne dlhý paket. Napr. IPv4 umožňuje pakety sekať - *fragmentácia paketov*, IPv6 definuje protokol na získanie MTU pre danú cestu a ponecháva na klientovi, aby zistil a dodržal túto hodnotu (inak bude jeho paket aj tak zahodený).

4.7 Efektívny prenos malých správ

??? V dnešnej dobe, keď sa jeden klik klávesy pri SSH prenáša pomocou HTTP paketu? (Asi 1000 násoboný overhead).

4.8 Multiplexovanie a demultiplexovanie

Pozri 2.6. Demultiplexovanie je inverznou operáciou.

4.9 Smerovanie (routing)

Široká téma Routing. Popísané v 13.5.

5 Rozhrania a služby

Sieťová služba (network service) - služby dostupné na sieti pre počítače pripojené na sieť. Často poskytujú zdielané zdroje a nazývajú sa aj port, daemon alebo listener. K službe sa pristupuje transportnými protokolmi. Sieťové rozhranie (network interface controller) - používa sa na pripojenie k sieti. Napr. sieťová karta. Používajú aktívne čakanie na prijímanie paketov (Plachetka approved polling).

5.1 Vzťah medzi vrstvami a rozhraniami

??? Asi na akých vrstvách sieťové rozhrania komunikujú. Na najnižšej, zabezpečujú prenos dát na fyzickej vrstve.

5.2 Service Access Points (SAP's)

Koncové body v sieti, ktoré majú svoj identifikátor (asi). NSAP adresy v OSI sú podobné IP adresám. Identifikujú koncové body v sieti, ku ktorým sa pristupuje protokolom ATM (Asynchronous Transfer Mode, unifikuje prenos v dátových a telekomunikačných sieťach). ATM prenáša celly, ktoré majú fixnú veľkosť (narozdiel od rámcov a paketov v IP).

5.3 Interface Data Unit (IDU)

Pod týmto menom som to poriadne nenašiel. Tvári sa to ako gateway (z IP), ktorý premosťuje viaceré protokoly (konverzia dát) a umožňuje prístup k iným sieťam.

5.4 Spojované a nespojované služby

??? Nechápem.

5.5 Kvalita služby a službové primitíva

??? Náhodný generátor kľúčových atribútov kvality:

- Spoľahlivosť.
- Bezpečnosť.
- Rýchlosť.
- Jednoduchosť.
- Užitočnosť.

6 Referenčné modely

Všeobecná definícia *referenčných modelov* v technickom svete: An abstract framework or domain-specific ontology consisting of an interlinked set of clearly defined concepts produced by an expert or body of experts in order to encourage clear communication. Laicky ide o všeobecné pravidlá architektúry systémov. Napr. von Neumannova architektúra počítača (CPU, Pamäť, ...). Alebo napr. taký *feng-shui* je referenčným modelom pre zariadenie domu. Pre každú miestnosť špecifikuje, ako by mala vyzerať (a hlavne ako nie) a tieto koncepty prepája medzi sebou (napr. záchod a kuchyňa by nemali susedieť).

6.1 Ciele a nebezpečenstvá

Náhodný generátor kľúčových atribútov cieľov a nebezpečenstiev (sú to protiklady):

- Jednoduchosť - ako v matematickej logike, chceme mať čo najmenej pravidiel. Ak budú globálne uznávané a používané, tak nie je problém systémy navrhnuté podľa referenčného modelu kombinovať, resp. je jednoduchšie pochopiť a navrhnúť nové systémy.
- Transparentnosť - aj fyzik, ktorý sa chce uživiť programovaním, by tomu mal pochopiť.
- Užitočnosť - špecifikuje niečo reálne a väčšinou už používané.
- Nebezpečenstvo - nedodržať ciele (napr. navrhnút tutti-frutti referenčný model, ktorý bude takým molochom, že sa tým nikto nebude riadiť).

6.2 Open Systems Architecture

Nemýliť si s OAS (Open Architecture Systems), používané Microsoftom, Citrix a VMware. Vrstvový referenčný model pre telekomunikácie. Jedna z implementácií spoločnosťou Boeing. Presn/ špecifikáciu som nenašiel, zakladá sa na OSI.

6.3 Norma ISO 7498 (jedna z generácií OSI)

Určený pre všetky telekomunikačné siete a protokoly.

Daná vrstva zahŕňa protokoly s podobnými funkcionalitami a cieľmi. Každá vrstva využíva len funkcie susedných vrstiev.

- Aplikačná. Komunikácia medzi procesmi, majú špecializovanú úlohu (OSI definuje striktnejšie, IP zahŕňa aj Presentation a Session). DNS, FTP, HTTP, SMTP, DHCP.
- Prezentačná (občas nazývaná aj Syntax layer). Odbremeňuje koncové aplikácie od rôznych reprezentácií posielaných dát (znakových reťazcov), napr. z dôvodu rôzneho kódovania koncových operačných systémov (ASCII, UTF, EBCDIC[3]). Môže sa tu používať šifrovanie / dešifrovanie (aj keď nie nutne, napr. IPsec a VPN na sieťovej vrstve). SSL/TLS, MIME (Multipurpose Internet Mail Extensions).
- Session. Umožňuje koncovým aplikáciám (procesom) na koncových zariadeniach udržiavať stav spojenia (nie presne, pozri Session), napr. login na webstránkach. Využíva sa v RPC (Remote procedure calls - volanie procedúr koncových procesov) alebo pri streamovaní videa, aby zvuk nepredbiehal obraz a naopak. SOCKS, Named Pipe.
- Transportná. Sprístupnenie end-to-end komunikácie pre aplikácie, môže zabezpečovať spoľahlivosť, dátové prúdy a multiplexovanie. TCP, UDP.

[3] Extended Binary Coded Decimal Interchange Code (EBCDIC) is an 8-bit character encoding used mainly on IBM mainframe and IBM midrange computer operating systems.

- Sieťová. Adresný priestor, smerovanie (routing) medzi koncovými stanicami. IP, ICMP, IPSec.
- Dátová. Vytváranie / posielanie základných logických jednotiek (postupnosti bitov) medzi fyzickými zariadeniami. Rámce (Frame), Switch, ATM (vytvára vituálne obvody)
- Fyzická. Kabeláž. USB, Bluetooth, Wifi (IEEE 802.11).

Poznamenajme, že v skutočnosti je prvou hlavičkou hlavička fyzickej vrstvy.

7 TCP/IP

Zoznam vrstiev a protokolov v TCP/IP referenčnom modely.

7.1 Referenčný model

Pozri 6.

TCP/IP. Okrem vrstiev špecifikuje aj konkrétne protokoly. *Internet* tu neznamená konkrétny Internet, ale medzi-sieť. Je špecializovaný na prenos binárnych dát. Daná vrstva zahŕňa protokoly s podobnými funkcionalitami a cieľmi. Každá vrstva využíva len funkcie susedných vrstiev.

- Aplikačná. OSI + IMAP, POP, SOCKS, SSH.
- Transportná. Prenos dát medzi koncovými zariadeniami. Rovnaké ako OSI.
- Sieťová (Internet Layer). Adresácia a komunikácia medzi viacerými lokálnymi sieťami. IP (adresovanie), ICMP (reponse codes), IPsec.
- Linková. Kábeláž pre lokálne siete. MAC (6bytové adresy zariadení (sieťových kariet)). ARP (kto má MAC adresu s danou IP?), Ethernet, DSL, ISDN.

Poznamenajme, že v skutočnosti je prvou hlavičkou hlavička linkovej vrstvy.
Patrí sa porozprávať o jednotlivých protokoloch.

7.2 Porovnanie a kritika OSI a TCP/IP referenčných modelov

OSI - Open systems interconnection. IP - Internet[4] Protocol suite. Oba modely delia komunikáciu na abstraktné vrstvy.

IP je novší, špecializovaný na prenos digitálnych dát a používa sa prakticky vo všetkých počítačových sieťach (asi). IP možnosť interpertovať ako inštanciu OSI.

Kritika: niečo pohaluzím.

8 Teoretické základy pre dátovú komunikáciu

Asi netreba vedieť, stačí tušiť. Ide o výsledky teórie informácie, ktorými sa zaoberá aj predmet Teória kódovania. Ide o širokú tému.

[4] Nie ten konkrétny

8.1 Nyquistovo tvrdenie (Nyquist–Shannon sampling theorem)

Veta (Shannova verzia). Nech $x(t)$ je vlnová funkcia[5] frekvencie v čase. Ak $(\forall t)x(t) \leq B$, tak je kompletne určená pomocou hodnôt vzdialených $\frac{1}{2B}$.

Ľudsky povedané, ak zachytávame vlnové signály, ktoré majú maximálnu frekvenciu B, tak nám stačí merať aktuálnu frekvenciu signálu každých $\frac{1}{2B}$. Naše merania potom jednoznačne určujú vlnovú funkciu $x(t)$.

V praxi vieme namerať diskrétne hodnoty spojitého signálu, ktoré podľa spomínanej vety vieme rekonštruovať naspäť na spojitú funkciu (niečo ako interpolačné polynómy - pre tých, čo mali numeriku).

8.2 Shannonove odhady a ich dôsledky

Odhady mám pass. Tipol by som, že frekvencie signálov v sieťových spojeniach sú nastavené tak, aby sa stíhali čítať. Alebo z druhej strany, cielená prenosová rýchlosť určuje frekvenciu priameho spojenia. Používa sa napr. aj v digitálnych fotoaparátoch.

9 Dátové prenosy

- *Sériová komunikácia.* Po komunikačnom kanály sa naraz posiela iba jeden bit informácie. Jeden kábel, jeden bit. Výhodou je jednoduchosť a cena.
- *Paralelná komunikácia.* Po komunikačnom kanály sa naraz posiela viacero bitov informácie. Kanál pozostáva z viacerych prenosových médií (káblov). Nevýhodou sú problémy so synchronizáciou, napr. kvôli zachovania poradia dát je nutné čakať na všetky bity v jednej dávke (Clock skew) alebo Crosstalak, keď signál v jednom kábli ovplyvňuje signály v okolitých kábloch (nedostatočné tienenie). Výhodou je teoreticky vyššia prenosová rýchlosť.

V minulosti sa sériová komunikácia používala hlavne na veľké vzdialenosti (cost-effective oproti paralelej) a paralelná na menšie (high-throughput). Sériové sa kvôli jednoduchosti (a dnešným prenosovým rýchlostiam) používajú aj na krátke vzdialenosti, napr serial bus (zbernica), alebo PCI (paralel) na PCI Express (serial). Sériové spojenia je možné pretaktovať na rádovo vyššie rýchlosti ako paralelné.

9.1 UART (Universal asynchronous receiver/transmitter)

Konverzia medzi sériovým a paralelným prenosom. Asynchrónne sériovo - každý bit je prenášaný v 8bitovom bloku, ktoré sú rozdelené start (nasleduje 8 butov) a stop (poslaných 8 bitov) signálmi. Dáta zo sériových prenosov sa buffrujú, aby sa potom mohli poslať paralelne. Používa sa v integrovaných obvodoch, materských doskách, sériových portoch, modemoch... .

9.2 USRT (Universal Synchronous Receiver-Transmitter)

Nepotrebuje start / stop signály, hodiny (clock) sú synchronizované rovnakou časovou jednotkou. UART podporujúci USRT sa nazýva USART (universal synchronous/asynchronous receiver/transmitter). Moderné UART majú podporu pre synchrónny mód.

9.3 Synchronizácia

In synchronous transmission, the clock data is recovered separately from the data stream and no start/stop bits are used. This improves the efficiency of transmission on suitable channels since more of the bits sent are usable data and not character framing. An asynchronous transmission sends no characters over the

[5] Poskladaná z konečného počtu sínusov a kosínusov. Záujemcovia nech si prečítajú Fourier transform.

interconnection when the transmitting device has nothing to send; but a synchronous interface must send "pad"characters to maintain synchronization between the receiver and transmitter. The usual filler is the ASCII "SYN"character. This may be done automatically by the transmitting device.

10 Elektromagnetické spektrum a bezdrôtové prenosy

Mám pass.

11 Prenosové média a sieťové komponenty

Mám dosť pass, nie som predsa fiitkár.

11.1 Techniky prepojovania sietí

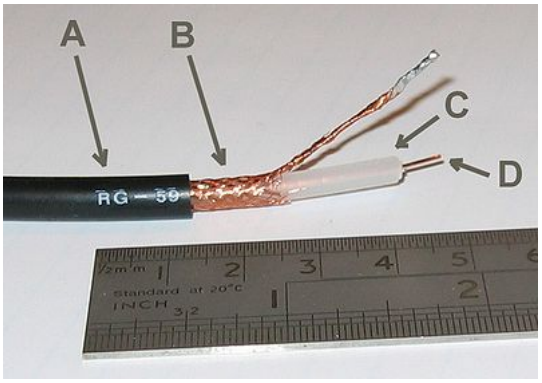
Asi rôzne topológie.

11.2 Charakter kabeláže

Sivá, biela, čierna.

11.3 Štruktúrovaná kabeláž

Koaxiálny kábel.



- A - Vonkajší plastový obal.
- B - Medené tienidlo (pred vesmírnym šumom).
- C - Elektrický izolátor.
- D - Medené jadro - prenosové médium.

Je ich asi 10 typov.

11.4 Sieťové zariadenia

- Gateway - konverzia dát medzi rôznymi sieťovými protokolmi, prístupový / výstupový bod siete. Používa vrstvy 4-7 OSI modelu.
- Hub - fyzicky je centrom hviezdicovej fyzickej topológie (ethernetové káble). Hub preposiela správu od každého každému a vytvára tak jednu kolíznu doménu. Logickú topológiu má teda zbernicovú. Druhá vrstva OSI.
- Bridge - rámce s adresou (MAC adresou[6]) nepreposiela každému. Ak adresu nepozná, tak sa spýta všetkých, koho adresa je (niečo ako ARP). Ďalej si už adresu pamätá (ak sa dlho nepoužila, môže ju zmazať). Druhá vrstva OSI.
- Switch - konceptuálne rovnaké ako bridge. Rozdiel je v tom, že switch skúma iba hlavičku prechádzajúcich rámcov, bridge kontroluje aj integritu (checksum). Druhá vrstva OSI. Rozdiely medzi bridgeom a switchom.
- Router - pozri 13.5.
- Repeater - zosilňuje signály a porušené signály znovu posiela. Prvá vrstva OSI.
- Proxy server - prostredník komunikácie (man in the middle). Cieľom je uľahčiť komunikáciu pre odosielateľa správy. Najvyššia vrstva.
- Firewall - monitoruje hlavičky paketov na sieťovej vrstve a na základe ich adries a portov sa rozhoduje, či komunikáciu prepošle ďalej, blokuje (a pošle dôvod prečo, napr. ICMP) alebo zahodí (a má pass zdôvodnenie).

  Bezstavový firewall má len takéto pravidlá. *Stavový* firewall si vie pamätať vytvorené virtuálne spojenia (ako napr. TCP). To je nutné v prípade, že klient vytvára virtuálny okruh a očakáva odpoveď, ktorú by bezstavový firewall odmietol (stavový si pamätá vytvorený virtuálny okruh a dovolí spätnú správu). Stavový firewall sa používa čo najbližšie ku koncovému užívateľovi (keď počet TCP spojení môže byť obrovský a pamäť je konečná - je nutné premazávať).

  Blacklist - niektorým zakáže, whitelist - len niektorým povolí.
- Network address translsator (NAT) - pozri praktiká zo sietí. Prepisuje adresy a porty v hlavičkách paketov. Účelom môže byť skrytie privátnych adries[7] za jednu verejnú (vytvoreným TCP spojeniam je možné pamätať si koncové adresy a porty). Takýto nat sa nazýva aj SNAT (source NAT). Existuje aj DNAT (destination NAT), ktorý pomocou port-forwardingu sprístupňuje privátne služby verejnosti (služba publikuje verejnú IP adresu a špeciálny port, povie to DNATu a ten mu preposiela komunikáciu zo zvoleného portu). Ak protokol nevytvára virtuálne okruhy, tak SNAT nevie pracovať stopercentne (keďže nevie, komu má preposielať spätné správy).
- Sieťová karta - každý vie.
- Modem (modulátor-demodulátor) - transformuje analógový signál na digitálny a naopak. V prípade Internetu sa využíval na pripojenie pomocou telefónnych liniek (dial-up).

[6] Bond, James Bond.
[7] Privátne adresy sa nemôžu vyskytnúť na Internete (konkrétny).

12 Linková vrstva (IP)

12.1 MAC adresa (Media Access Control address)

Unikátny identifikátor pre sieťové zariadenia (sieťové karty napr.), dodávané ich výrobcom. Má 6 byteov, prvé tri pre výrobcu (OUI - Organizationally Unique Identifier), ďalšie tri pre unikátny identifikátor (NIC - Network interface controller). Špeciálne $FF:FF:FF:FF:FF:FF$ je broadcastová adresa.

MAC - Media Access Control - akým spôsobom sa pristupuje k zdielanému médiu (na ktorom môže vysielať viacero staníc naraz).

12.2 IEEE štandardy 802 pre LAN (a WAN)

Február 1980. Rôzne veľkosti paketov. Rozdeľuje dátovú vrstvu na MAC (predošlý odstavec) a LLC - Logical Link Control, ktorý umožňuje viacerým rôznym protokolom "paralelný"prístup k médiu (komunikačný kanál).

Je ich viacero, napr.:

- 802.3 Ethernet
- 802.11 Wireless LAN
- 802.15.1 Bluetooth

12.3 FDDI (Fiber Distributed Data Interface)

Sieťová karta. Umožňuje prenos 100Mbit/s, na kružnicovej topológií (zdielané médium). Používal sa v LAN. Nahradený Fast Ethernet.

12.4 Fast Ethernet

Lacný, všade používaný (nazývaný aj LAN kábel). 100Mbit / s. Hviezdicová topológia (centrom je Hub, Switch alebo Router). Používa CSMA/CD (Detekcia kolízií s náhodným čakaním (podľa exponenciálnej distribúcie pravdepodobnosti = *exponential backoff*) v prípade kolízie). Viacero verzií podľa druhu vodiča (medené / optické).

12.5 Gigabit Ethernet

Od roku 2010 "common and economical"(štandardizované 1998). Pomocou switchov je umožnená full-duplex komunikácia (obojsmerná). Zas asi 10 verzií (od 25m po 70 km), (asi vždy) optické vlákna.

12.6 10 Gigabit Ethernet

Len full-duplex (obojsmerne), nedá sa použiť s hubmi ani s CSMA/CD. Od roku 2002. Problémom sú 10Gbit routre (podľa istých zdrojov realizovateľné na moderných grafických kartách, lepšie ako bitcoiny). Optické káble. Zas kopa verzií, typovo rovnakých.

12.7 802.11 (Wireless LAN)

Pozri Cviká z počítačových sietí, ďalej len výcuc. CSMA (Carrier Sense Multiple Access - Collision avoidance) - ak je linka obsadená, tak exponential backoff. Zdielané médium - 2.4GHz až 5GHz pásma. Antény ovplyvňujú kvalitu. Viacero protokolov (rôzne prenosové rýchlosti).

Stanica (Station) je zariadením vo WiFi sieti. BSS (Basic Service Set) - zariadenia, ktoré vedia medzi sebou komunikovať v dvoch režimoch:

- *Ad-hoc* režim, alebo tiež IBSS (Independent Basic Service Set) sa používa v prípade, keď je treba jednoduchým spôsobom vytvoriť bezdrôtovú sieť. Prvá stanica vytvárajúca sieť náhodne zvolí BSSID, začne vysielať majáčiky (beacons) oznamujúce prítomnosť siete a ostatné stanice komunikujú priamo medzi sebou. Ak stanice dlhšiu dobu nedostanú beacon, predpokladajú, že prvá stanica vypadla a zvyšné stanice v náhodnom čase začnú vysielať beacony (prvá stanica vyhráva).
- *Infrastructure* režim obsahuje stanicu, ktorá zároveň plní úlohu prístupového bodu – AP (Access Point), s ktorou komunikujú všetky ostatné stanice (dve stanice môžu vždy komunikovať iba cez AP).

Problém s bezpečnosťou (ľahké zachytávania paketov). Zabezpečenie:

- Bez šifrovania – najstarší, najjednoduchší, najnebezpečnejší.
- WEP (Wired Equivalent Privacy). Šifra RC4 (64-128bitový)
- WPA (Wi-Fi Protected Access). Namiesto RC4 TKIP (Temporal Key Interchange Protocol) - časté menenie kľúčov (neprichádza k celkovému odhaleniu komunikácie pri odhlení jedného kľúča).
- WPA2. Novšia verzia.
- EAP (používaný aj v point-to-point). Má oveľa širšie možnosti autentifikácie (meno/heslo, certifikát, ...).

Distribučný systém - prepojenie viacerých WiFi routrov (staníc) medzi sebou Ethernetom alebo bezdrátovo. Treba myslieť na MAC adresy, keďže nemusia byť pod daným routrom.

Mesh networking (také peer-to-peer). Každý je rovnocenný, preposiela pakety ďalej (chová sa ako wifi router). Nie je rozšírené.

12.8 802.15 (Wireless PAN)

PAN - personal area network - len medzi zariadenia používané jednou osobou (napr.:mobil, tablet, notebook, desktop, mp3 player) - nazýva sa aj *Body Area Network*. Bluetooth, WiFi (staré infraporty a ďalšie).

12.9 802.16 (Wireless broadband)

Ako mobilná sieť, ale ponúka bezdrátové pripojenie k Internetu. Viac na Broadband Wireless Access.

12.10 Bluetooth

Výmena dát na krátku vzdialenosť. Každý pozná. Dosť komplikovaná implementácia.

13 Sieťová vrstva (OSI)

Dôležitá otázka. Dobre popísané v praktikách zo sietí. Je ekvivalentná internet layer v IP. Cieľom vrstvy je, aby vedeli počítače medzi sebou komunikovať bez ohľadu na použitie konkrétnej linkovej vrstvy (ethernet, WiFi, dial-up, ISDN, ADSL, ...).

Odporúčam pozrieť si niečo o IPsec (AH a ESP).

13.1 Interná organizácia sieťovej vrstvy

Hlavnými cieľmi sú:

- Nevytvárať virtuálne okruhy. Zaručuje iba end-to-end komunikáciu.
- Adresný priestor. Každý užívateľ siete má unikátnu adresu (nemusí byť pravda v prípade použitia NATu).
- Smerovanie správy. Nie každý vie priamo posielať správy hocikomu po linkovej vrstve, keďže nemusia byť spojení káblom. Preto sa správa musí posielať cez viacero vrstiev - smerovanie (niečo ako GPS).

13.2 Príklad prenosu packetov cez sieť

Routre s routovacími tabuľkami. Dve prepojené siete.

13.3 Uzly a smerovacie tabuľky

Uzly ???. Asi sa myslia sieťové zariadenia, ktoré sú spojené s viacerymi sieťovými zariadeniami (hub, switch, router, NAT, ...). Smerovacie tabuľky v 13.5.

13.4 IP protokol

Suverénne najpoužívanejší protokol. Aktuálne sa prechádza na IPv6 (128bitové adresy), kvôli vyčerpaniu adresného priestoru IPv4 (32bitové adresy).

Fragmentácia. IP definuje pohyblivú veľkosť packetu (po 2^16). Použité linkové vrstvy môže mať rôzne obmedzenia na veľkosť paketu. Preto IPv4[8] umožňuje packety v uzloch *fragmentovať* - rozdeliť. Ďalší uzol potom tieto pakety spojí naspäť. *MTU* - Maximum transport unit - označuje maximálnu veľkosť paketu prenositeľného cez vytvorený virtuálny okruh (alebo spojenie).

Adresácia. IPv4 adresy sú 4 bajtové, zapisujú sa 123.45.67.255. Spolu s ňou sa posiela *sieťová maska* (subnet mask), ktorá rozdeľuje adresu na *adresu siete* (network identifier) a *adresu zariadenia* (host identifier). Maska je niekoľko jednotiek nasledovaných nulami (32 možností), píše sa ako číslo udávajce počet jednotiek za IP adresu: 123.45.67.255/24.

IP vyhradzuje špeciálne adresy. 127.0.0.1 je loopback (localhost) a pre lokálne použitie 10.0.0.0/8, 172.16.0.0/12 a 192.168.0.0/16. Broadcastová adresa vznikne ako adresa siete vyplnená jednotkami: $123.0.0.1/8 \mapsto 123.255.255.255$ alebo $158.195.213.69/8 \mapsto 158.195.213.255$. Adresy môžu byť staticky nastavené (administrátorom), alebo získané dynamicky (pomocou DHCP, pozri 15.1) (dá sa určite nastaviť vo vašom obľúbenom operačnom systéme).

ARP. IP adresy musia byť v konečnom dôsledku preložené na MAC adresy. Na tento účel slúži protokol *ARP - Address Resolution Protocol*. Prebieha v dvoch fázach. Najprv uzol pošle broadcast všetkým na sieti s otázkou "Who has IPadresa?". Dotyčné zariadenie odpovedá svojou MAC adresou. Uzol si zobrazenie $IPaddress \mapsto MACaddress$ môže istý čas pamätať.

ICMP (Internet Control Message Protocol). Kontrolná správa. Prenáša len jeden flag - status. Napr. firewall môže poslať ICMP v prípade, že správu blokoval.

[8] IPv6 fragmentáciu zakazuje, je nutné dopredu zistiť MTU (resp. použiť minimálnu).

Time to live. Môže sa stať, že routovacie tabuľky môžu tvoriť cykli (resp. nevedia doručiť daný paket). Preto IP definuje TTL položku, ktorá určuje maximálny počet skokov, ktorý môže paket v sieti urobiť.

13.5 Smerovanie

Ide o to doručiť správy v prípade, že medzi komunikujúcimi zariadeniami neexistuje priame spojenie.

Spôsoby doručenia.

- Unicast - správa je určená jednému konkrétnemu.
- Broadcast - správa je určená všetkým v sieti (neposiela sa ďalej medzi siete - internetwork).
- Multicat - správa sa posiela množine vrcholov.
- Anycast - správa sa doručuje práve jednému z množiny vrcholov (najčastejšie najbližšiemu).

Používané zariadenia.

- Router. Pomocou *routovacej tabuľky* $adresa_prijemcu \mapsto preposlat_na$ smeruje správy ďalej, resp. určenému príjemcovi.
- Bridge. Príjemcu hľadá pomocou floodingu - opýta sa každého v sieti (napr. protokol ARP 13.4, resp Neighbor Discovery v IPv6). Keď našiel, tak si ho zapamätá. Používa sa v malých sieťach, ako najnižší router.
- Gateway (nazývané aj protocol converters). Ich hlavným účelom je konverzia dát medzi dvoma protokolmi, resp. sú vstupnými bránami do iných $\{\epsilon$,pod,nad$\}$sietí. Využívajú sa na ľubovoľnej vrstve.
- Firewall. Preposiela, Zahadzuje (ničí) alebo Blokuje (pošle echo prečo) správy na základe jednoduchých pravidiel (port, protokol, IP adresa). Pracuje na sieťovej vrstve. Viac o firewalloch v 11.4.
- Switch. Narozdiel od hubu (kotrý preposiela správy všetkým ostatným), posiela správu len jej príjemcovi.

Routovacie tabuľky.

- Statické. Administrátor siete natvrdo zadá, kadiaľ sa majú preposielať dáta určené pre danú adresu.
- Adaptívne. Vo veľkých dynamických sieťach (napr. Internet) nie je možné konfigurovať staticky, preto si routre medzi sebou pravidelne vymieňajú informácie (každý router pozná zopár iných, napr. štandardný domáci router pozná router ISP).

Algoritmy na vypĺňanie routovacích tabuliek:

- Distance vector algorithms - Bellman-Ford ($O(n^3)$). Každej hrane sa priradí cena, potom zbehne algoritmus na výpočet vzdialeností (násobenie matice susednosti), správy od routra R pre A sa smerujú po najkratšej ceste. Tento prístup sa využíva v malých (lokálnych) sieťach. Môže sa použiť aj zložitejší Dijsktrou algoritmus, ale pre niektoré zariadenia môže byť príliš zložitý.
- OLSR - Optimised Link State Routing - prehľadáva sa len do hĺbky 2, používa sa v ad-hoc sieťach (netreba vedieť).
- Path vector protocol - vytvorí sa hierarchická štruktúra, každý vrchol je zodpovedný za svojich priamych potomkov, použije sa hierarchická adresácia. Táto hierarchická štruktúra je updateovaná pomocou špecializovaných protokolov (RFC-1322). Používa s v medzisieťovom smerovaní.

13.6 CIDR (Classless Inter-Domain Routing)

Do roku 1993 boli všetky adresy rozdelené len do piatich tried a susediace adresy nemuseli susediť aj topologicky. Od roku 1993 CIDR rozdeľuje adresy na adresu siete a adresu zariadenia (maska siete, spomínané vyššie).

Dosahuje sa tak jednoduchší routing (stačí poslať správu sieti) a rozširuje sa potenciálny počet IPv4 adries (koncové zariadenia nemusia mať unikátnu adresu, NAT).

13.7 Tunelovanie

Pozri cviká zo sietí.

Účelom tunelu je vytvoriť virtuálne spojenie, cez ktoré sa dá komunikovať tak, akokoby boli koncové zariadenia spojené priamo. Prakticky sa paket P (hocijakej vrstvy) zabalí do špeciálneho tunelovacieho paketu - obalu (sieťová vrstva). Obal sa medzi sieťami prenáša, prechádza cez routre, firewally, NAT, proxy, ... (ktorým sa P takýmto spôsobom úspešne vyhýba). Ak dosiahne router v koncovej sieti, tak sa rozbalí a P sa pošle, akokeby vznikol na tej koncovej sieti.

Výhody tunelovania sú, že je možné celý paket poslať bezpečne po sieti. Je možné zabezpečiť autenticitu (kto paket posielal), hlavičku a obsah (šifrovaním) a integritu (checksum). To v bežných paketoch nie je možné v takej miere, lebo niektoré časti sa pri prechode cez routre menia (TTL, header checksum,...).

VPN (Virtual private network) pozri Wikipédiu. Tunelovaním sa vytvára virtuálna lokálna sieť, ktorá spája množinu klientov. Títo klienti posielajú potom medzi sebou správy, akokeby boli na izolovanej fyzickej sieti (akékoľvek správy, nie je možné odpočúvať, vieme zaručiť kto správu poslal a či sa zmenila). VPN sú populárne, nemôže chýbať v každej modernej firme. Jednou z implementácií je OpenVPN.

14 Transportná vrstva (IP, OSI)

Dôležitá otázka. Pozri praktiká z počítačových sietí.

Cieľom transportnej vrstvy je zabezpečiť transparentný prenos dát medzi ľubovoľnými dvoma používateľmi (procesmi) v sieti. Keďže na jednom počítači môže bežať viac procesov, úlohou transportnej vrstvy je aj umožniť paralelný prenos viacerých prúdov dát. Protokoly to riešia tak, že rozšíria sieťové adresy o ďalší prvok - čislo portu. Adresa na transportnej vrstve je potom tvaru (sieťová adresa, číslo portu) a jednoznačne identifikuje tzv. socket cez ktorý komunikuje nejaký proces.

14.1 UDP (User Datagram Protocol)

Najjednoduchší. Nezabezpečuje pratkicky nič, len sa snaží správu doručiť (aspoň raz). Rozširuje IP hlavičku iba o čísla portov a checksum. Používa sa, keď nie je spoľahlivosť doručenia požiadavkou. Napr. streamovanie porna, keď nám až tak nevadí, keď sa niektoré pakety stratia. Používa sa aj pri tunelovaní.

14.2 TCP (Transmission Control Protocol)

Pozri praktiká z počítačových sietí [9].

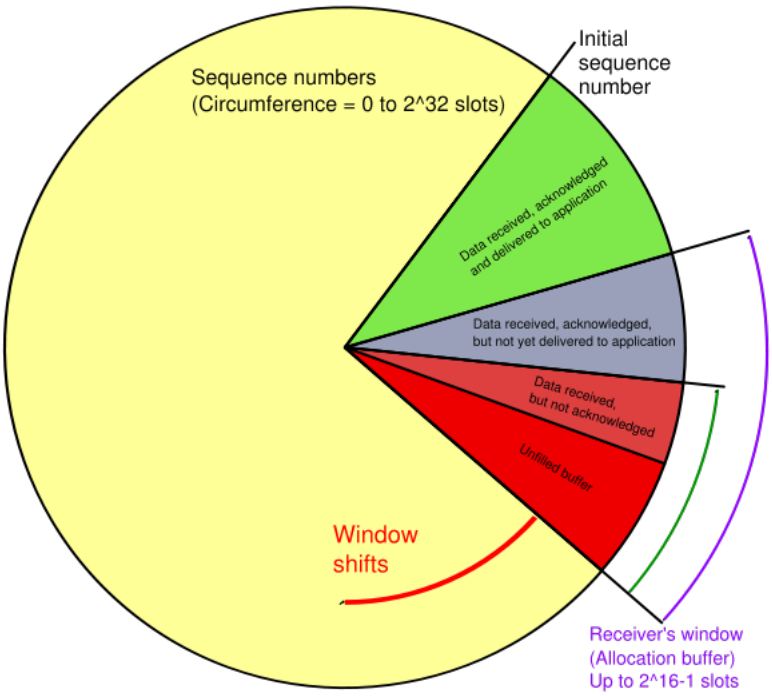
Transmission control protocol (TCP) je najpoužívanejším protokolom transportnej vrstvy na Internete. Služby ako World Wide Web (HTTP protokol), e-mail (protokoly SMTP, POP3, IMAP) a mnohé iné používajú TCP na prenos údajov. Vytvára virtuálne okruhy pre prenos prúdu dát a zaručuje spoľahlivosť prenosu (preposielanie stratených a preusporiadanie doručených). Príjemca potvrdzuje príjem.

[9] Väčšina textu tejto sekcie (TCP) je skopírovaná z danej stránky, dúfame, že sa tým neporušili žiadne copyrighty.

Hlavička

Offset (bajt)	Popis
0-1	Číslo zdrojového portu (Source port)
2-3	Číslo cieľového portu (Destination port)
4-7	Poradové číslo (Sequence number)
8-11	Potvrdzujúce číslo (Acknowledgment number (if ACK set))
12-13	Príznaky
14-15	Veľkosť okna (Window Size)
16-17	Kontrolný súčet (Checksum)
18-19	Smerník na urgentné dáta (nepoužívané) (Urgent pointer (if URG set))
20-...	Voliteľné rozšírenia (Options)

Poradové číslo určuje do ktorej časti prúdu patria dáta, ktoré sa prenášajú v danom segmente. Na základe tohto poľa vie príjemca poskladať segmenty prijaté v nesprávnom poradí, prípadne zistiť, že niektoré dáta neprijal resp. prijal viackrát. Na začiatku spojenia sa toto pole určí ľubovoľne (nezávisle pre každý smer komunikácie) a následne sa zväčšuje s každým prenesením bajtom.



Príjemca oboznamuje odosielateľa, že úspešne prijal dáta tým, že vyšle vlastný TCP segment v ktorom nastaví potvrdzujúce číslo na hodnotu o jeden väčšiu ako poradové číslo posledného prijatého bajtu (t.j. potvrdzujúce číslo má hodnotu poradového čísla, ktorú príjemca očakáva ako nasledovnú).

Vytváranie, riadenie a ukončovanie spojenia.

Bit	Popis
0-3	Smerník na dáta
4-7	Rezervované
8	Congestion Window Reduced (CWR)
9	ECN-Echo (ECE)
10	Smerník na urgentné dáta je platný (URG)
11	Potvrdzujúce číslo je platné (ACK)
12	Push (PSH)
13	Resetovanie spojenia (RST)
14	Synchronizovanie poradových čísel (SYN)
15	Žiadne ďalšie údaje od odosielateľa (FIN)

PSH - vykonaj ihneď a nebufruj správy na príjemcovej strane. RST - ukončenie spojenia. SYN - inicializuje TCP spojenie (three way handshake) a SYNchronizuje poradové čísla, príjemca odpovedá SYN a ACK. Spojenie sa ukončuje FIN.

Nečaká sa na potvrdenie (ACK) každého paketu (veľmi veľmi pomalé), posiela sa aj viacero paketov naraz (sliding window).

Kontrola zahltenia (Congestion control) TCP obsahuje viacero mechanizmov, ktorými sa snaží zabrániť zahlteniu siete. Každá strana si udržuje tzv. "congestion window", čo je odhad maximálneho množstva dát, ktoré sa môžu poslať súčasne (bez čakania na potvrdenie) bez výpadkov.

Okno sa na začiatku exponenciálne zväčšuje, kým nepríde k výpadku, vtedy sa resetuje.

14.3 SSL/TLS

Šifrovanie určené pre transportnú vrstvu (SSL je staršia verzia). Asymetrické šifrovanie pre výmenu kľúčov (štandardne Diffie-Hellman), symetrické šifrovanie pre nečitateľnosť a MAC na integritu a autenticitu[10] (napr. podpisovaním hashu správy). Rozširuje štandardné protokoly ako HTTP, IMAP, ... na HTTPS, IMAPS, ...

Zjednodušený priebeh protokolu:

- Odosielateľ (klient) a príjemca (server) si vymenia informácie o nastaveniach.
- Klient overí autenticitu servra (môže aj servert klienta). Ak nemá zapamätaný jeho verejný kľúč, tak konzultuje certifikačné autority.
- Klient sa dohodne so serverom na spoločnom tajomstve pre túto komunikáciu (pomocou DH protokolu). Šifruje verejným kľúčom servra.
- Zo spoločného tajomstva sa vygenerujú session keys, ktorými sa správy ďalej šifrujú.
- Potvrdí sa session key.
- Môže sa bezpečne komunikovať.

Certifikačné autority. Aby klient vedel overiť autenticitu, musí veriť spojeniu verejný kľúč - IPadresa. Viera (trust) týchto dvojíc je outsourcovaná na *certifikačné* autority, ktoré podpisujú takéto certifikáty. Certifikačné autority tvoria stromovú štruktúru. Koreňu stromu sa implicitne verí. Certifikát, ktorý nie je registrovaný CA je neplatný a všetky prehliadače na to upzorňujú.

[10] Istota, že správu vytvoril naozaj užívateľ s danou IP adresou.

15 Aplikačná vrstva a podporné protokoly

Dôležitá otázka.

Protokoly určené na špecializovanú komunikáciu medzi procesmi (process-to-process).

15.1 DHCP (Dynamic Host Configuration Protocol)

Pozri praktiká z počítačových sietí.

Protokol slúži na získanie IP adresy v lokálnej sieti. Pri úvodnom pripojení klient nemá IP adresu a potrebuje nejakú získať. Kontaktuje preto DHCP server UDP paketom na adresu 255.255.255.255 (a port 67) so zdrojovou adresou 0.0.0.0[11] s obsahom DHCPDISCOVER, v ktorej uvádza svoju MAC adresu a zoznam nastavení.

Vo všeobecnosti server odpovedá broadcastom[12] DHCPOFFER (na port 68) a navrhuje aspoň jednu IP adresu, z ktorej si klient vyberie a oznámi broadcastom DHCPREQUEST a nastaví si IP stack. Server odpovie unicastom DHCPACK.

15.2 DNS (Domain Name System)

Pozri praktiká z počítačových sietí.

Distribuovaná databáza bijektívneho zobrazenia znakových reťazcov (dómen) a IP adries. Jedny sa ľahko pamätajú ľudom, druhé počítačom. Priestor doménových mien je strom, pričom každý vrchol toho stromu môže mať priradené rôzne typy záznamy. Koreň stromu sa označuje bodkou. Každému vrcholu stromu (okrem koreňa) je priradené meno pozostávajúce z písmen, číslic a pomlčky.

DNS servre (nameservre) tvoria hierarchickú stromovú štruktúru. Každý z nameservrov má na starosti svoju zónu. Pre každú zónu existuje aspoň jeden hlavný (master) NS a podriadený (slave) si záznamy kopírujú (kvôli distribuovanému prístupu).

Položky DNS záznamu:

- Meno. Plné meno vrcholu ku ktorému sa viaže daný záznam, získané zreťazením mien všetkých vrcholov na ceste ku koreňu, pričom jednotlivé mená oddeľujeme bodkou.
- Trieda. Najzaujímavejšia trieda je IN (internet), ešte sú definované aj triedy CN (chaos) a HS (hesiod).
- Typ:
  - A,AAAA - autoritatívne záznamy. Tento nameserver je za ne zodpovedný.
  - PTR - opačný preklad (ip na name).
  - NS - delegovanie autority na iný nameserver (presmerovanie).
  - MX - mail exchange - mailový server.
  - SOA - start of authority - popisuje údaje o samotnej zóne.
- TTL - dokedy je záznam platný a môže sa cacheovať.
- Ďalšie dáta.

Dva režimy pracovania DNS servra:

- Nerekurzívny. DNS server vracia len autoritatívne záznamy (A), ak nemá záznam, tak vráti čiastočný výsledok: NS záznam ukazujúci na nameserver, ktorý má viac informácií (klient sa potom rekurzívne pýta).

[11] Je to trocha hack, posielať IP pakety, keď ešte IP stack nebol inicializovaný.
[12] Keďže klient ešte nemá nakonfigurovaný IP stack.

- Rekurzívny. DNS server sa sám rekurzívne pýta ostatných nameserverov na odpoveď.

Odpovede sa môžu cacheovať, maximálne ale TTL čas. DNS je na porte 53, pristupuje sa UDP alebo TCP.

15.3 HTTP (Hypertext Transfer Protocol)

Request-response, client-server. Skoro každá webová komunikácia ide cez HTTP, keďže firewally nezvyknú blokovať port 80.

15.4 SSH (Secure Shell)

Secure Shell (SSH) is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively).

15.5 FTP (File Transfer Protocol)

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server.

Komunikácia nie je šifrovaná a veľa webhostingov nepodporuje šifrovanú verziu SFTP. Odporúča sa preto používať SCP, ak sa dá.

15.6 SMTP (Simple Mail Transfer Protocol)

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use SMTP for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP).

Tiež len štruktúra, zabezpečenie napr. PGP.

16 Telefónny systém

Naozaj len v krátkosti (už nemám silu písať).

The public switched telephone network (PSTN) is the network of the world's public circuit-switched telephone networks. It consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all inter-connected by switching centers, thus allowing any telephone in the world to communicate with any other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core and includes mobile as well as fixed telephones.

16.1 Modemy

Modem (modulátor-demodulátor) - transformuje analógový signál na digitálny a naopak. V prípade Internetu sa využíval na pripojenie pomocou telefónnych liniek (dial-up).

16.2 Štandardy

??? Tých je určite kopa.

16.3 Konštelačné vzorky

??? Google mi vyhľadá iba súhvezdia a iné konštelácie.

16.4 Modulačné techniky

Česká wikipédia je fajná.

16.5 ISDN - systém pre domáce a firemné využitie

ISDN je zkratka z anglického termínu Integrated Services Digital Network, český název pro tuto síť je Digitální síť integrovaných služeb.

Dnešní telefonní sítě jsou založeny na digitálních telefonních ústřednách a přenosové cesty mezi ústřednami jsou také plně digitalizovány. Poslední analogová část sítě tak zůstává účastnická přípojka. Tedy poslední část od ústředny k telefonnímu přístroji (modemu, faxu atd.) účastníka. ISDN nabízí plně digitální přenos až k účastníkovi (A/D a D/A převod signálu se odehrává přímo v koncovém přístroji). ISDN dále nabízí možnost komunikovat pomocí jedné digitální účastnické přípojky pomocí hlasu, textu a obrazu. Obecně pak mluvíme o multimediální komunikaci. ISDN přípojku lze pomocí takzvaného terminálového adaptoru (TA) nesprávně „ISDN modem“ samozřejmě použít také pro připojení do sítě Internet.

16.6 xDSL, B-ISDN

DSL (anglicky Digital Subscriber Line) je technologie, která umožňuje využít stávající vedení telefonu nebo kabelové televize pro vysokorychlostní přenos dat. Využívá telefonní rozvody plochým nekrouceným kabelem, kroucenou dvojlinku nebo koaxiální kabel kabelové televize. Jednotlivé typy DSL se liší v používaném frekvenčním pásmu, maximální rychlosti a dosahu. Obecně platí že čím větší vzdálenost od ústředny nebo méně kvalitní vedení, tím nižší maximální dosažitelná rychlost.

Pro běžné domácí nasazení se obvykle využívá asymetrická varianta (ADSL), kde je vyšší přenosová rychlost ve směru k zákazníkovi (anglicky download) a nižší rychlost směrem od zákazníka (anglicky upload). Ve firemním prostředí se používají symetrické varianty, kde jsou obě rychlosti stejné.

17 Diaľkové vedenia a multiplexovanie, optické siete

Tiež len v krátkosti (už nemám silu písať). Je to rôznych spôsoboch využívania frekvenčného pásma.

17.1 FDMA/TDMA/CDMA

V tejto sekcií popisujeme Multiple Access systémy, ktoré riešia problém, keď viacerý užívatelia chcú naraz využívať zdieľané médium na komunikáciu.

Frequency Division Multiple Access or FDMA is a channel access method used in multiple-access protocols as a channelization protocol. FDMA gives users an individual allocation of one or several frequency bands, or channels. It is particularly commonplace in satellite communication. FDMA, like other Multiple Access systems, coordinates access between multiple users In FDMA all users share the satellite simultaneously but each user transmits at single frequency. FDMA can be used with both analog and digital signal.

Time Division Multiple Access paralelizuje digitálnu komunikáciu tak, že každému užívateľu vyhradí krátky *time slot* na jeho prenos. Užívatelia sa striedajú (pozri operačné systémy a scheduling).

17.2 Synchrónne optické siete (SDH, SONET architektúra - definícia rámcov v SDH)

Synchrónne optické siete = Synchronous Optical Networking (SONET) ≈ Synchronous Digital Hierarchy (SDH). Standardized multiplexing protocol that transfer multiple digital bit streams over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs).

Výhodou oproti Ethernetu je, že je možné prenášať dáta na veľké (medzištátne) vzdialenosti.

Definícia rámca na wikipédií. Prenosová rýchlosť 155.52 Mbit/s a jeden rámec sa prenesie za 125 microsekúnd (125×10^{-6} sekúnd).

18 Referencie a odporúčaná literatúra

- `http://en.wikipedia.org`.
- `http://netlab.dcs.fmph.uniba.sk/siete/`.
- `http://www.dcs.fmph.uniba.sk/~plachetk/TEACHING/DISTRSYS2012/siete.pdf`.
- Nepoužil som, mali by upresňovať low-level veci: `http://fmfi-uk.hq.sk/Informatika/Pocitacove%20Siete/`.